日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　２月　６日

出願番号
Application Number: 特願２００３－０２８９９８

[ST. 10/C]: [ＪＰ２００３－０２８９９８]

出願人
Applicant(s): 株式会社ルネサステクノロジ

２００４年　２月１７日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

【書類名】　特許願
【整理番号】　K03000561A
【あて先】　特許庁長官殿
【国際特許分類】　G06F 12/00
【発明者】
【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
【氏名】　水島　永雅
【発明者】
【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
【氏名】　角田　元泰
【発明者】
【住所又は居所】　東京都小平市上水本町五丁目２０番１号　株式会社日立製作所半導体グループ内
【氏名】　片山　国弘
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社　日立製作所
【代理人】
【識別番号】　100075096
【弁理士】
【氏名又は名称】　作田　康夫
【手数料の表示】
【予納台帳番号】　013088
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1

【物件名】　　要約書　1

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　メモリカード

【特許請求の範囲】

【請求項１】

複数のブロックに分割されたメモリと、前記メモリへのアクセスを制御するコントローラと、ＩＣカードチップを備えたメモリカードにおいて、

前記コントローラは、外部のホスト機器からの第１のコマンドに応答して、前記メモリのブロックの利用権を、前記ＩＣカードチップによって実行されるべきアプレットのために前記アプレットごとに割り当て、

前記コントローラは、前記ホスト機器からの第２のコマンドに応答して、前記第１のコマンドに応答した処理を実行可能なアンロック状態から前記第１のコマンドに応答した処理を拒否するロック状態へ遷移するメモリカード。

【請求項２】

請求項１に記載のメモリカードにおいて、

前記メモリは、前記ブロックの識別子と前記ブロックの利用権が割り当てられたアプレットの識別子との対応を管理するための管理情報を記憶可能で、

前記コントローラは、前記アンロック状態である場合に、前記管理情報の内容の変更を許可し、

前記コントローラは、前記ロック状態である場合に、前記管理情報の内容の変更を禁止するメモリカード。

【請求項３】

請求項１に記載のメモリカードにおいて、

前記メモリは、前記ブロックの識別子と前記ブロックの利用権が割り当てられたアプレットの識別子との対応を管理するための管理情報を記憶可能で、

前記コントローラは、前記ブロックの利用権を前記アプレットのために割り当てる場合に、前記ブロックの識別子に対応する前記アプレットの識別子を前記管理情報に追加するメモリカード。

【請求項４】

請求項１に記載のメモリカードにおいて、

前記メモリは、前記第１のコマンドに応答した処理を実行可能か否かを識別するためのフラグを記憶可能で、

前記コントローラは、前記アンロック状態から前記ロック状態へ遷移する場合に、前記フラグの値を変更するメモリカード。

【請求項５】

請求項１に記載のメモリカードにおいて、

前記コントローラは、前記ホスト機器からの第３のコマンドに応答して、前記ロック状態から前記アンロック状態へ遷移するメモリカード。

【請求項６】

請求項５に記載のメモリカードにおいて、

前記メモリは、前記第３のコマンドに応答した処理を許可するための参照パスワードを記憶可能で、

前記コントローラは、前記ホスト機器から受け取ったパスワードと前記メモリ内の前記参照パスワードとが一致した場合に、前記第３のコマンドに応答して、前記ロック状態から前記アンロック状態へ遷移するメモリカード。

【請求項７】

請求項１に記載のメモリカードにおいて、

前記コントローラは、前記ホスト機器からの第４のコマンドに応答して、前記アプレットのために割り当てられた前記ブロックの利用権を解除するメモリカード。

【請求項８】

請求項７に記載のメモリカードにおいて、

前記メモリは、前記ブロックの識別子と前記ブロックの利用権が割り当てられたアプレットの識別子との対応を管理するための管理情報を記憶可能で、

前記コントローラは、前記アプレットのために割り当てられた前記ブロックの利用権を解除する場合に、前記ブロックの識別子に対応する前記アプレットの識別子を前記管理情報から削除するメモリカード。

【請求項９】

請求項１に記載のメモリカードにおいて、

前記メモリは、前記ホスト機器から受け取ったデータを記憶するための第１のエリアと、前記アプレットのために前記ブロックの利用権が割り当てられた第２のエリアとを有するメモリカード。

【請求項１０】

請求項９に記載のメモリカードにおいて、

前記コントローラは、前記メモリの前記第２のエリアへ書き込むべきデータを前記ＩＣカードチップから受信し又は前記第２のエリアから読み出されたデータを前記ＩＣカードチップへ送信するための転送コマンドを前記アプレットごとに生成するメモリカード。

【請求項１１】

複数のブロックに分割されたメモリと、前記メモリへのアクセスを制御するコントローラと、ＩＣカードチップを備えたメモリカードにおいて、

前記メモリのブロックは、前記ＩＣカードチップによって実行されるアプレットのために前記アプレットごとに割り当てられ、

前記メモリは、前記ＩＣカードチップが前記コントローラへ依頼する外部処理の内容を前記コントローラが前記ＩＣカードチップへ問い合わせるために前記アプレットごとに定められたコマンドを記憶可能で、

前記ＩＣカードチップは、当該ＩＣカードチップが実行すべきアプレットの識別子を前記コントローラへ送出し、

前記コントローラは、前記ＩＣカードチップからの前記アプレットの識別子をキーとして、前記メモリから前記コマンドを読み出し、読み出された前記コマンドを前記ＩＣカードチップへ送出し、

前記ＩＣカードチップは、前記コントローラからの前記コマンドに応答して、前記外部処理の内容を前記コントローラへ通知し、

前記コントローラは、前記ＩＣカードチップからの通知に応答して、前記外部処理を実行するメモリカード。

【請求項１２】

請求項１１に記載のメモリカードにおいて、

前記コマンドは、前記メモリのブロックへ書き込むべきデータを前記ＩＣカー

ドチップから前記コントローラへ転送するための第１の転送コマンドと、前記メモリのブロックから読み出されたデータを前記コントローラから前記ＩＣカードチップへ転送するための第２の転送コマンドとを含むメモリカード。

【請求項１３】

請求項１１に記載のメモリカードにおいて、

前記コマンドは、前記アプレットごとに異なり、さらに、外部のホスト機器からのコマンドと異なるメモリカード。

【請求項１４】

ＩＣカードチップと、メモリと、前記メモリへのアクセスを制御するコントローラとを備えたメモリカードにおいて、

前記メモリは、外部のホスト機器からのデータを記憶するための第１の記憶エリアと前記ＩＣカードチップからのデータを記憶するための第２の記憶エリアを有し、

前記第２の記憶エリアは、複数のブロックに分割され、

前記各ブロックは、前記ＩＣカードチップによって実行されるべきアプレットのために前記アプレットごとに割り当てられ、

前記コントローラは、前記ホスト機器からのコマンドに応答して前記第１の記憶エリアをアクセスし、

前記コントローラは、前記ＩＣカードチップからのコマンドに応答して前記第２の記憶エリアをアクセスするメモリカード。

【請求項１５】

請求項１４に記載のメモリカードにおいて、

前記メモリは、前記ブロックの識別子と前記ブロックの利用権が割り当てられたアプレットの識別子との対応を管理するための管理情報を記憶可能であり、

前記コントローラは、前記アプレットの識別子を前記ＩＣカードチップから受信し、受信された前記アプレットの識別子をキーとして前記ブロックの識別子を前記管理情報から決定し、決定された前記ブロックの識別子によって特定されたブロックをアクセスするメモリカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、セキュリティ機能を搭載した記憶装置及びその記憶装置が挿入可能なホスト機器及びその記憶装置を備えたホスト機器に係り、フラッシュメモリチップとコントローラチップとＩＣカードチップを有するメモリカード等に関する。

【０００２】

【従来の技術】

特許文献１には、ＩＣモジュールと大容量のフラッシュメモリを搭載するメモリカードが記載されている。

【０００３】

特許文献２には、アプリケーションプログラムごとの実行必須条件をＩＣカードに記憶させておき、処理要求があった時に実行必須条件を充足していれば実行可能とし、充足していなければ実効不能とすることが記載されている。

【０００４】

特許文献３には。ＩＣカード内のメモリ領域のうち、銀行のために領域Ａが、病院のために領域Ｂが、それぞれ割り付けられていることが記載されている。

【０００５】

【特許文献１】特開平10-198776号公報

【特許文献２】特開2000-66882号公報

【特許文献３】特開平6-222980号公報

【０００６】

【発明が解決しようとする課題】

しかし、何れの従来技術も、ＩＣカードのアプリケーションプログラム（アプレット）ごとに、分割された記憶エリアを割り当てることまでは記載されていない。よって、従来技術では、各アプリケーションプログラムが互いのメモリ内のデータを不正に侵害することが懸念される。

【０００７】

本発明の目的は、ＩＣカードチップのアプレット間のデータ干渉、即ち、一の

アプレットに割り当てられたメモリが他のアプレットにもアクセスされてデータが侵害されることを抑制できる記憶装置を提供することである。

【０００８】

【課題を解決するための手段】

本発明は、メモリを複数のブロックに分割し、ブロックの使用権をＩＣカードチップのアプレットごとに割り当てた。つまり、メモリが、ホスト機器からのデータを記憶するための第１の記憶エリア（例えば、ノーマルデータエリア）とＩＣカードチップからのデータを記憶するための第２の記憶エリア（例えば、セキュアデータエリア）を有し、さらに、第２の記憶エリアが複数のブロックに分割され、さらに各ブロックがアプレットごとに割り当てられる。

【０００９】

また、本発明は、ホスト機器からコマンドによって、ブロックの使用権の割り当て、割り当て解除、割り当て及び解除の禁止、割り当て及び解除の禁止の解除を行うようにした。つまり、本発明は、ホスト機器からの第１のコマンド（例えば、アプレット登録コマンド）に応答してメモリのブロックの利用権をアプレットごとに割り当て、ホスト機器からの第２のコマンド（例えば、管理テーブルロックコマンド）に応答してアンロック状態からロック状態へ遷移する。さらに、ホスト機器からの第３のコマンド（例えば、管理テーブルアンロックコマンド）に応答してロック状態からアンロック状態へ遷移し、ホスト機器からの第４のコマンド（例えば、アプレット登録解除コマンド）に応答してアプレットのために割り当てられたブロックの利用権を解除する。

【００１０】

また、本発明は、ＩＣカードチップがコントローラへ依頼する外部処理の内容をコントローラがＩＣカードチップへ問い合わせるためのコマンドを、アプレットごとに規定した。

【００１１】

【発明の実施の形態】

以下、本発明の一実施形態について説明する。

【００１２】

図１は、本発明を適用したＭｕｌｔｉＭｅｄｉａＣａｒｄ（ＭｕｌｔｉＭｅｄｉａＣａｒｄはＩｎｆｉｎｅｏｎＴｅｃｈｎｏｌｏｇｉｅｓＡＧの登録商標である。以下、「ＭＭＣ」と略記する。）の内部構成図を簡単に表したものである。ＭＭＣ１１０は、ＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠するのが好ましい。ＭＭＣ１１０は、外部に接続したホスト機器１６０がＭｕｌｔｉＭｅｄｉａＣａｒｄのプロトコル仕様に準拠したメモリカードコマンドを発行することによって、ファイルデータを読み書きすることができるストレージ機能や、機密データ保護や個人認証などに必要な暗号演算をおこなうことができるセキュリティ処理機能を有する。ホスト機器１６０は、例えば、携帯電話、携帯情報端末（ＰＤＡ）、パーソナルコンピュータ、音楽再生（及び録音）装置、カメラ、ビデオカメラ、自動預金預払器、街角端末、決済端末等が該当する。ＭＭＣ１１０は、ＭＭＣ外部端子１４０、コントローラチップ１２０、フラッシュメモリチップ１３０、ＩＣカードチップ１５０を持つ。フラッシュメモリチップ１３０は、不揮発性の半導体メモリを記憶媒体とする大容量（例えば、６４メガバイト）のメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。ＭＭＣ外部端子１４０は７つの端子から構成され、外部のホスト機器１６０と情報交換するために、電源供給端子、クロック入力端子、コマンド入出力端子、データ入出力端子、グランド端子を含む。コントローラチップ１２０は、ＭＭＣ１１０内部の他の構成要素（ＭＭＣ外部端子１４０、フラッシュメモリチップ１３０、ＩＣカードチップ１５０）と接続されており、これらを制御するマイコンチップである。ＩＣカードチップ１５０は、ＩＣカードのプラスチック基板中に埋め込むためのマイコンチップであり、その外部端子、電気信号プロトコル、コマンドはＩＳＯ／ＩＥＣ７８１６規格に準拠している。ＩＣカードチップ１５０の外部端子には、電源供給端子、クロック入力端子、リセット入力端子、Ｉ／Ｏ入出力端子、グランド端子がある。ＩＣカードチップ１５０の外部端子は、グランド端子を除いて、電源供給端子、クロック入力端子、リセット入力端子、Ｉ／Ｏ入出力端子がコントローラチップ１２０に接続されている。コントローラチップ１２０は、ＩＣカードチップ１５０の外部端子からＩＣカードチップ１５０にＩＣカードコマンドを発行することによって、外部のホスト機器１６０から要求されたセ

キュリティ処理に必要な演算をおこなう。ＩＣカードチップ１５０は、演算処理を行うためのＣＰＵ１５１と、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）１５２とを備える。一方、フラッシュメモリチップ１３０には、記憶素子を備えるが、マイコンは存在しない。

【００１３】

セキュリティ処理は、例えば、ＩＣカードチップ１５０内のＥＥＰＲＯＭ１５２にデータが書き込まれるとき、又は、ＥＥＰＲＯＭ１５２からデータが読み出されるときにＣＰＵ１５１により実行される。セキュリティ処理の詳細な内容は、ＥＥＰＲＯＭ１５２内に格納されたプログラムコードによって記述されている。多種多様なセキュリティ処理に適用できるように、そのプログラムコードは機能的に異なる複数のモジュールとして構成されている。ＣＰＵ１５１は必要に応じてセキュリティ処理に使用するモジュールを切り替えることができる。以下、このモジュール単位をアプレットと呼ぶ。例えば、ＥＥＰＲＯＭ１５２は、アプレットＡ１５３とアプレットＢ１５４とを格納する。ＥＥＰＲＯＭ１５２の記憶容量は例えば６４キロバイトであり、フラッシュメモリチップ１３０の記憶容量より小さい。但し、本発明を実施する上で、ＥＥＰＲＯＭ１５２の記憶容量は、フラッシュメモリチップ１３０の記憶容量と同じでもよいし、大きくてもよい。

【００１４】

ＩＣカードチップ１５０には、セキュリティ評価基準の国際標準であるＩＳＯ／ＩＥＣ１５４０８の評価・認証機関によって認証済みである製品を利用する。一般に、セキュリティ処理をおこなう機能を持つＩＣカードを実際の電子決済サービスなどで利用する場合、そのＩＣカードはＩＳＯ／ＩＥＣ１５４０８の評価・認証機関による評価と認定を受ける必要がある。ＭＭＣにセキュリティ処理をおこなう機能を追加することによってＭＭＣ１１０を実現し、それを実際の電子決済サービスなどで利用する場合、ＭＭＣ１１０も同様にＩＳＯ／ＩＥＣ１５４０８の評価・認証機関による評価と認定を受ける必要がある。ＭＭＣ１１０は、評価・認証機関によって認証済みのＩＣカードチップ１５０を内蔵し、そのＩＣカードチップ１５０を利用してセキュリティ処理をおこなう構造を持つことによ

り、セキュリティ処理機能を得る。したがって、ＭＭＣ１１０はＩＳＯ／ＩＥＣ１５４０８に基づくセキュリティ評価基準を容易に満足することができ、ＭＭＣにセキュリティ処理機能を追加するための開発期間を短縮することができる。

【００１５】

ＭＭＣ１１０は、ＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した外部インタフェースを持つのが好ましい。ＭＭＣ１１０は、一種類の外部インタフェースを通じて、ＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した標準メモリカードコマンドに加えて、セキュリティ処理を実行するコマンド（以下、セキュアライトコマンドと呼ぶ。）を受け付ける。セキュアライトコマンドは入力データを伴う。コントローラチップ１２０は、ＭＭＣ１１０が受信したコマンドが標準メモリカードコマンドであるか、セキュアライトコマンドであるかによって、アクセスすべきチップを選択し、コマンド処理を分配する機能を持つ。標準メモリカードコマンドを受信したならば、フラッシュメモリチップ１３０を選択し、これにフラッシュメモリコマンドを発行してホストデータを読み書きできる。また、セキュアライトコマンドを受信したならば、ＩＣカードチップ１５０を選択し、これにＩＣカードコマンドを発行してセキュリティ処理を実行することができる。ここで発行されるＩＣカードコマンドは、セキュアライトコマンドによって入力されるデータ（以下、セキュアライトデータと呼ぶ。）の中に埋め込まれている。ＩＣカードチップ１５０はこのコマンドに応じてＩＣカードレスポンスを返すが、コントローラチップ１２０はそれをキャッシュする。さらに、ＭＭＣ１１０は、一種類の外部インタフェースを通じて、セキュリティ処理の結果を読み出すコマンド（以下、セキュアリードコマンドと呼ぶ。）も受け付ける。セキュアリードコマンドは出力データを伴う。セキュアリードコマンドを受信したならば、キャッシュしておいたＩＣカードレスポンスを含むデータ（以下、セキュアリードデータと呼ぶ。）を出力する。

【００１６】

図５は、セキュアライトデータおよびセキュアリードデータのフォーマットの一例を示したものである。このフォーマットは、実行するセキュリティ処理の内容が１つのＩＣカードコマンドで表現でき、セキュリティ処理の結果が１つのＩ

Ｃカードレスポンスで表現できる場合に適用することが好ましい。上述の通り、ＩＣカードチップ１５０に送信するＩＣカードコマンド、ＩＣカードチップ１５０から受信するＩＣカードレスポンスはともにＩＳＯ／ＩＥＣ７８１６－４規格に従う。本規格によれば、ＩＣカードコマンドの構成は、４バイトのヘッダ（クラスバイトＣＬＡ、命令バイトＩＮＳ、パラメータバイトＰ１とＰ２）が必須であり、必要に応じて、入力データ長指示バイトＬｃ、入力データフィールドＤａｔａＩｎ、出力データ長指示バイトＬｅが後に続く。また、ＩＣカードレスポンスの構成は、２バイトのステータスＳＷ１とＳＷ２が必須であり、必要に応じて、出力データフィールドＤａｔａＯｕｔがその前に置かれる。本フォーマットにおけるセキュアライトデータ５０１は、ＩＣカードコマンド５０２の前にＩＣカードコマンド長Ｌｃａ５０４を付け、さらにＩＣカードコマンド５０２の後にダミーデータ５０５をパディングしたものである。Ｌｃａ５０４の値はＩＣカードコマンド５０２の各構成要素の長さを合計した値である。一方、セキュアリードデータ５１１は、ＩＣカードレスポンス５１２の前にＩＣカードレスポンス長Ｌｒａ５１４を付け、さらにＩＣカードレスポンス５１２の後にダミーデータ５１５をパディングしたものである。Ｌｒａ５１４の値はＩＣカードレスポンス５１２の各構成要素の長さを合計した値である。なお、この図では、ＩＣカードコマンドにＬｃ、ＤａｔａＩｎ、Ｌｅが含まれ、ＩＣカードレスポンスにＤａｔａＯｕｔが含まれる場合のフォーマット例を表している。ＭＭＣ１１０に対する標準メモリカードコマンドに含まれるデータリード／ライトコマンドの仕様では、リード／ライトアクセスするデータを固定長のブロック単位で処理することが基本となっている。よって、セキュアライトデータ５０１やセキュアリードデータ５１１のサイズも、ＭＭＣ１１０の標準メモリカードコマンドの仕様に準拠したブロックサイズに一致させることが好ましい。ダミーデータ５０５、５１５は、セキュアライトデータ５０１やセキュアリードデータ５１１のサイズをブロックサイズに一致させるために適用される。ブロックサイズとして採用する値は、一般の小型メモリカードが論理ファイルシステムに採用しているＦＡＴ方式におけるセクタサイズ（５１２バイト）が望ましい。パディングするダミーデータ５０５、５１５は全てゼロでもよいし、乱数でもよいし、コントローラチップ１２０や

ホスト機器１６０がデータエラーを検出したり訂正するためのチェックサムでもよい。Ｌｃａ５０４の値はコントローラチップ１２０がセキュアライトデータ５０１からダミーデータ５０５を除去してＩＣカードコマンド５０２を抽出するために使用し、Ｌｒａ５１４の値はホスト機器１６０がセキュアリードデータ５１１からダミーデータ５１５を除去してＩＣカードレスポンス５１２を抽出するために使用する。

【００１７】

コントローラチップ１２０は、電源供給端子、クロック入力端子を通して、ＩＣカードチップ１５０への電源供給、クロック供給を制御する。ホスト機器１６０からセキュリティ処理を要求されないときには、ＩＣカードチップ１５０への電源供給やクロック供給を停止させることができ、ＭＭＣ１１０の電力消費を削減することができる。

【００１８】

電源供給されていないＩＣカードチップ１５０を、ＩＣカードコマンドを受信できる状態にするには、まず、ＩＣカードチップ１５０に電源供給を開始し、リセット処理を施すことが必要である。コントローラチップ１２０は、ＭＭＣ１１０がホスト機器１６０からセキュアライトコマンドを受信したのを契機に、電源供給端子を通してＩＣカードチップ１５０への電源供給を開始する機能を持つ。また、コントローラチップ１２０は、ＭＭＣ１１０がホスト機器１６０からセキュアライトコマンドを受信したのを契機に、リセット入力端子を通してＩＣカードチップ１５０のリセット処理をおこなう機能を持つ。コントローラチップ１２０は、セキュアライトコマンドを受信するまでＩＣカードチップ１５０への電源供給を停止させておくことができる。したがって、ＭＭＣ１１０の電力消費を削減することができる。

【００１９】

コントローラチップ１２０は、ＩＣカードチップ１５０のクロック入力端子を通してＩＣカードチップ１５０に供給するクロック信号をＭＭＣ１１０内部で発生し、その周波数、供給開始タイミング、供給停止タイミングを制御する機能を持つ。ＭＭＣ外部端子１４０のクロック入力端子のクロック信号と無関係にする

ことができるため、ホスト機器１６０によるタイミング解析、電力差分解析、故障利用解析と呼ばれる攻撃法に対してセキュリティが向上する。

【００２０】

フラッシュメモリチップ１３０は、ノーマルデータエリア１３１と管理エリア１３２とセキュアデータエリア１３３とを含む。

【００２１】

ノーマルデータエリア１３１は、セクタ単位に論理アドレスがマッピングされている領域であり、ホスト機器１６０が標準メモリカードコマンドを使用することにより指定した論理アドレスにデータを読み書きできる領域である。

【００２２】

セキュアデータエリア１３３は、ＩＣカードチップ１５０内のＥＥＰＲＯＭ１５２に格納されたアプレット（例えば、１５３や１５４）をＣＰＵ１５１が実行する際に（すなわち、セキュリティ処理を実行する際に）、扱うデータを格納することができる領域である。セキュアデータエリア１３３は複数のブロックに分割されている。これをセキュアデータブロックと呼ぶ。例えば、セキュアデータエリア１３３は４つのセキュアデータブロック１３３ａ、１３３ｂ、１３３ｃ、１３３ｄで構成される。セキュアデータブロックは、コントローラチップ１２０がアプレットごとにその利用権を割り当てることができる単位である。例えば、アプレットＡ１５３はセキュアデータブロックｃ１３３ｃの利用権を持ち、アプレットＢ１５４はセキュアデータブロックａ１３３ａの利用権を持つ。また、各セキュアデータブロックは複数の固定長データレコードに分割されている。例えば、１レコードのサイズは１２８バイトであり、１つのセキュアデータブロック当たり８１９２個のレコードで構成される。このとき、１つのセキュアデータブロックのサイズが１メガバイトとなり、セキュアデータエリア１３３の容量は４メガバイトとなる。したがって、ＥＥＰＲＯＭ１５２に格納されたアプレットは、セキュアデータエリア１３３に格納されたデータにアクセスすることによって、ＥＥＰＲＯＭ１５２の容量以上の不揮発データを利用できる。例えば、ＩＣカードチップ１５０内のアプレットＡ１５３が電子決済に関するセキュリティ処理のためのプログラムである場合、決済ログ（支払金額や日時など）をセキュアデ

ータエリア１３３に格納することにより、ＥＥＰＲＯＭ１５２のみを利用するよりも多くの決済ログが保存でき、ユーザの利便性が高くなる。ＩＣカードチップ１５０からセキュアデータエリア１３３へのアクセス方法の詳細は後に述べる。

【００２３】

一方、管理エリア１３２は、コントローラチップ１２０がセキュアデータエリア１３３を管理するための情報を格納する領域である。コントローラチップ１２０は、ＭＭＣ１１０がホスト機器１６０からセキュアライトコマンドを受信したことを契機に、この領域に情報を格納したり、削除したりする。そのコマンドについては後述する。管理エリア１３２は、ロックフラグ１３４とパスワードエリア１３５と管理テーブル１３６とを含む。

【００２４】

管理テーブル１３６は、セキュアデータエリア１３３を構成している各セキュアデータブロックの利用権を持つアプレットを登録するための領域である。アプレットを識別するために、この領域にアプリケーション識別子（以下、ＡＩＤ（Ａｐｐｌｉｃａｔｉｏｎ ＩＤｅｎｔｉｆｉｅｒ）と呼ぶ。）を格納することによってアプレットを登録することが望ましい。ＡＩＤは、ＩＣカードのアプリケーションプログラムを識別するために、国際的にユニークに割り振られた値を持つ。国際的に流通するＡＩＤの付番方法は、国際規格としてＩＳＯ／ＩＥＣ７８１６－５で規定されている。ＡＩＤを利用することにより、セキュアデータエリア１３３を使用するアプレットを確実に識別することができる。コントローラチップ１２０は、ＡＩＤ１３７に同一のＡＩＤを複数格納することを禁止する。管理テーブル１３６のブロックの欄は、セキュアデータブロックを識別するためのブロック識別子としてブロックの先頭アドレス値を登録する。但し、先頭アドレス値の代わりにＭＭＣ内でユニークな番号をブロック識別子として登録してもよい。尚、管理テーブル１３６の代わりに、各セキュアデータブロック内に直接にＡＩＤを登録）してもよい。

【００２５】

管理テーブル１３６には、ＡＩＤ１３７だけでなく、アプレットごとに転送コマンドコード１３８を格納することができる。この転送コマンドコード１３８は

、コントローラチップ１２０がセキュアデータブロックの利用権を、アプレットのために割り当てる時に、コントローラチップ１２０によって生成されるのは好ましい。転送コマンドコードとは、“ライト転送コマンド”および“リード転送コマンド”それぞれのコマンドＡＰＤＵ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ Ｄａｔａ Ｕｎｉｔ）のＣＬＡバイトとＩＮＳバイトに設定する２バイト×２個の値である。ここで、“ライト転送コマンド”および”リード転送コマンド”とは、セキュアデータエリア１３３にレコードデータをライトする前、あるいはそこからレコードデータをリードした後に、コントローラチップ１２０とＩＣカードチップ１５０との間でそのレコードデータを転送するために、コントローラチップ１２０がＩＣカードチップ１５０に対して発行するＩＣカードコマンド形式のコマンドである。特に、コントローラチップ１２０へレコードデータを送り出すためのコマンドをライト転送コマンドと呼び、ＩＣカードチップ１５０へレコードデータを送り込むためのコマンドをリード転送コマンドと呼ぶ。これらのコマンドの詳細な説明は後述する。セキュアデータエリア１３３の利用権を持つアプレット（１５３や１５４）には、ライト／リード転送コマンドを受信した際にレコードデータを扱う処理プログラムが記述されている。転送コマンドコード１３８はアプレットごとに個別に決められるようになっている。もし、転送コマンドコードが全てのアプレットに共通の固定値であるならば、ホスト機器１６０からのセキュアライトデータに含まれるアプレット特有のコマンドとライト／リード転送コマンドとの間でコーディングの競合が発生する可能性がある。本発明によれば、このようなコーディング競合を防ぐことができる。なお、転送コマンドコード１３８のうちＩＮＳコードに関しては、伝送プロトコルの都合上ＩＳＯ／ＩＥＣ７８１６－３に準拠していなければならない。

【００２６】

ロックフラグ１３４は、管理テーブル１３６に格納された登録情報の変更の可否を示す１バイトのデータを格納する領域である。この領域にＦＦｈを設定することで管理テーブル１３６の情報の変更が禁止状態（ロック状態）であることを示す。また、００ｈを設定することで管理テーブル１３６の情報の変更が許可状態（アンロック状態）であることを示す。

【００２７】

パスワードエリア１３５は、管理テーブル１３６の情報をアンロック状態にするための２５５バイトのパスワードの参照値を格納しておく領域である。管理テーブル１３６の情報をロックする時には必ず、ホスト機器１６０からセキュアライトコマンドにより、２５５バイトのパスワード参照をこの領域に設定する。管理テーブル１３６の情報をアンロック状態にする場合は、ホスト機器１６０からセキュアライトコマンドにより、ロック時に設定したパスワード参照と同じパスワードを入力する必要がある。入力したパスワードとパスワード参照との一致によって、管理テーブル１３６の情報の変更をアンロックすることができる。

【００２８】

管理エリア１３２は、ホスト機器１６０が不正にアクセスしてセキュリティ処理を解析することができないように、コントローラチップ１２０により物理的にアクセス制限がかけられている。つまり、管理エリア１３２はコントローラチップ１２０による論理アドレスが割り振られていないため、ホスト機器１６０が直接データを読み書きできない。したがって、ＭＭＣ１１０のセキュリティ処理の信頼性や安全性が向上する。

【００２９】

以下、図２を参照しながら、セキュアデータエリア１３３に対するレコードデータのライト／リードアクセスにおいて用いられるライト／リード転送コマンドのコマンドＡＰＤＵとレスポンスＡＰＤＵについて詳細に述べる。

【００３０】

図２ａは、ＩＣカードチップ１５０が出力するレスポンスＡＰＤＵを示している。このレスポンスＡＰＤＵ２００に含まれるＤａｔａＯｕｔ２０４の先頭２バイト（以下、先頭から順に第１制御バイト２０１、第２制御バイト２０２と呼ぶ。）、およびＳＷ１バイト２０５とＳＷ２バイト２０６に特別な値を設定することにより、ＩＣカードチップ１５０はコントローラチップ１２０にセキュアデータエリア１３３に対するアクセス要求を通知することができる。なお、後続出力データ２０３（ＤａｔａＯｕｔ２０４のうち第１制御バイト２０１と第２制御バイト２０２を除いた部分）は、アクセス要求に必要な情報を送信するために使用

される。

【００３１】

ＩＣカードチップ１５０は、コントローラチップ１２０に対してセキュアデータエリア１３３へアクセスすることを要求するため、ＳＷ１バイト２０５とＳＷ２バイト２０６に９０ＦＦｈという専用のステータス値を設定しなければならない。コントローラチップ１２０は、ＩＣカードチップ１５０が出力するレスポンスＡＰＤＵを常に監視し、ＳＷ１バイト２０５とＳＷ２バイト２０６の値が９０ＦＦｈであることを検出したら、その前方にあるＤａｔａＯｕｔ２０４の第１制御バイト２０１、第２制御バイト２０２第１制御バイト第２制御バイトを調査し、要求されたアクセスの内容などを認知する。一方、９０ＦＦｈでなかった場合は、このレスポンスＡＰＤＵを含むセキュアリードデータをホスト機器１６０に出力する。ただし、ＳＷ１バイト２０５とＳＷ２バイト２０６の値が９０ＦＦｈであっても、条件によって、そのままホスト機器１６０に出力されることがある。その詳細は後述する。

【００３２】

コントローラチップ１２０は、セキュアデータエリア１３３へのアクセスを開始するとき、ＩＣカードチップ１５０上で選択されているアプレットが何であるかによって、１３３ａ～１３３ｄの中からアクティブにするセキュアデータブロックを選択する。アクセスすべきセキュアデータブロックの選択は、ＩＣカードチップ１５０からアクセス開始要求が発生した直後におこなう。アクセス開始要求のためにＤａｔａＯｕｔ２０４に設定するデータの仕様を以下に示す。第１制御バイト２０１の上位４ビットには、０００１を設定する。第１制御バイト２０１の下位４ビットには、アクセスモードを示すコードを設定する。ここで指定可能なアクセスモードには、レコードデータのライト、レコードデータのリードの２種類がある。０００１というコードはレコードデータのライト、００１０というコードはレコードデータのリードである。その他のコードは無効である。また、後続出力データ２０３には、ＩＣカードチップ１５０上で選択されているアプレットのＡＩＤを設定する。第２制御バイト２０２には、そのＡＩＤの長さを設定する。

【００３３】

コントローラチップ１２０は、第１制御バイトの上位４ビットが０００１ならば、後続出力データ２０３に含まれるＡＩＤで管理テーブル１３６内の全てのＡＩＤ１３７を検索し、アクティブにすべきセキュアデータブロックを決定する。一致するＡＩＤが見つからなかった場合は、このレスポンスＡＰＤＵを含むセキュアリードデータをホスト機器１６０に出力する。ＡＩＤを検出し、それに対応するセキュアデータブロックが判明した後、コントローラチップ１２０は、第１制御バイトの下位４ビットが０００１ならばライト、００１０ならばリードのアクセスを開始すると認識する。第１制御バイトの下位４ビットがそれ以外の場合は、このレスポンスＡＰＤＵを含むセキュアリードデータをホスト機器１６０に出力する。

【００３４】

コントローラチップ１２０がアクセスモード（ライトまたはリード）を認知した後、そのモードに応じてライト／リード転送コマンドを発行することによって、アクティブなセキュアデータブロック対してライトすべきレコードデータ、またはリードしたレコードデータをＩＣカードチップ１５０とコントローラチップ１２０との間で転送することができる。図２ｂと図２ｃはライト／リード転送コマンドのコマンドＡＰＤＵを示したものである。図２ｂはコントローラチップ１２０からＩＣカードチップ１５０への転送データがない場合、図２ｃは転送データがある場合を示している。前述のように、ライト／リード転送コマンドのコマンドＡＰＤＵ２１０（または２２０）のＣＬＡバイト２１４（または２２６）とＩＮＳコード２１５（または２２７）にはあらかじめアプレットごとに登録されたものを設定する。そのため、管理テーブル１３６から２バイト×２個の転送コマンドコード１３８を読み出す。

【００３５】

ライト／リード転送コマンドのコマンドＡＰＤＵ２１０（または２２０）では、直前のアクセスの結果をＩＣカードチップ１５０に通知するため、Ｐ１バイト２１６（または２２８）とＰ２バイト２１７（または２２９）に特殊な値を設定する。０００００ｈは直前のアクセスにエラーがないことを意味する。８０ＸＸｈ

は直前のアクセスにエラーが発生したことを意味する。なお、ＸＸはエラー内容を示す１６進コードである。エラーの場合、アクティブなセキュアデータブロックへのデータアクセスは実行されない。よって、セキュアデータブロックのレコードデータの内容も変化しない。

【００３６】

ＩＣカードチップ１５０は、ライト／リード転送コマンドのレスポンスＡＰＤＵ２００における後続出力データ２０３を用いて、ライトしたいレコード番号とレコードデータ、またはリードしたいレコード番号をコントローラチップ１２０に送信する。ライトモードでは、指定レコード番号（４バイト）とライトデータ（１２８バイト）の連結データを設定し、リードモードでは、指定レコード番号（４バイト）を設定する。このように、後続出力データ２０３の長さはアクセスモードによって変わるので、ライト／リード転送コマンドのコマンドＡＰＤＵのＬｅバイト２１３（または２２５）には、アクセスモードに応じた値を設定する必要がある。ライトモードでは、後続出力データ２０３の長さが８４ｈとなるのでＤａｔａＯｕｔ２０４の長さは８６ｈとなる。よって、Ｌｅバイト２１３（または２２５）には８６ｈを設定する。リードモードでは、後続出力データ２０３の長さが０４ｈとなるのでＤａｔａＯｕｔ２０４の長さは０６ｈとなる。よって、Ｌｅバイト２１３（または２２５）には０６ｈを設定する。

【００３７】

アクセス開始直後の（つまり、最初に発行される）ライト／リード転送コマンドのコマンドＡＰＤＵは、図２ｂの形式となる。そのとき、Ｐ１バイト２１６とＰ２バイト２１７には、０００００ｈを設定する。Ｌｅバイト２１３には、ライトモードの場合８６ｈを、リードモードの場合０６ｈを設定する。

【００３８】

ライト／リード転送コマンドのレスポンスＡＰＤＵは、図２ａの形式をとる。ＩＣカードチップ１５０上で選択されているアプレットは、レスポンスＡＰＤＵ２００を利用してアクティブなセキュアデータブロックに対するアクセス（ライト／リード）をコントローラチップ１２０に要求することができる。以下、これをアクセス実行要求と呼ぶ。第１制御バイト２０１と第２制御バイト２０２に設

定するデータの仕様を以下に示す。第１制御バイト２０１の上位４ビットには、００１０を設定する。第１制御バイト２０１の下位４ビットには、要求するアクセスを示すコードを設定する。０００１というコードはレコードデータのライト、００１０というコードはレコードデータのリードである。その他のコードは無効である。このコードが表すアクセスモードは、コントローラチップ１２０が認めるアクセスモードに一致していなければならない。また、その第２制御バイト２０２によって、次回のアクセスモード（ライト／リード）の要求をおこなうことができる。コントローラチップ１２０はこれを参照して、自身が認めるアクセスモードをスイッチする。

【００３９】

コントローラチップ１２０は、第１制御バイト２０１の上位４ビットが００１０ならば、アクティブなセキュアデータブロックに対して、指定されたレコード番号のデータをライト／リードする。ライト／リード処理が正常終了した場合（アクセス結果２１２（または２２２）の値が０００００ｈ）、第２制御バイト２０２が０１ｈならば自身が認めるアクセスモードをライトモードにスイッチ、０２ｈならばリードモードにスイッチする。ライト／リード処理に何らかのエラーがあった場合（アクセス結果２１２（または２２２）の値が８０ＸＸｈ）、自身が認めるアクセスモードをスイッチせずにエラーが起きた時点のものを維持する。

【００４０】

コントローラチップ１２０が２回目以降に発行するライト／リード転送コマンドのコマンドＡＰＤＵは、直前のアクセスの結果やアクセスモードの状態遷移によって、図２ｂの形式になったり、図２ｃの形式になったりする。またＬｅ２１３（または２２５）の値も変わる。その詳細を以下に示す。

【００４１】

直前のライトアクセスが正常で次回もライトモードのとき、図２ｂの形式であり、アクセス結果２１２の値が００００ｈで、Ｌｅ２１３の値は８６ｈである。

【００４２】

直前のライトアクセスが正常で次回がリードモードのとき、図２ｂの形式であり、アクセス結果２１２の値が００００ｈで、Ｌｅ２１３の値は０６ｈである。

【００４３】

直前のリードアクセスが正常で次回もリードモードのとき、図２ｃの形式であり、アクセス結果２２２の値が０００００ｈで、Ｌｃ２２３の値は８０ｈで、ＤａｔａＩｎ２２４にはリードしたレコードデータが設定され、Ｌｅ２２５の値は０６ｈである。

【００４４】

直前のリードアクセスが正常で次回がライトモードのとき、図２ｃの形式であり、アクセス結果２２２の値が０００００ｈで、Ｌｃ２２３の値は８０ｈで、ＤａｔａＩｎ２２４にはリードしたレコードデータが設定され、Ｌｅ２２５の値は８６ｈである。

【００４５】

直前のライトアクセスがエラーのとき、図２ｂの形式であり、アクセス結果２１２の値が８０ＸＸｈで、Ｌｅ２１３の値は８６ｈである。

【００４６】

直前のリードアクセスがエラーのとき、図２ｂの形式であり、アクセス結果２１２の値が８０ＸＸｈで、Ｌｅ２１３の値は０６ｈである。

【００４７】

アクセスエラー時にアクセス結果２１２（または２２２）に設定する８０ＸＸｈにおいて、エラー内容を示すコードＸＸの例を以下に示す。

【００４８】

ＸＸ＝０１は、指定されたレコード番号がアクセス可能な範囲外であるエラーを意味する。

【００４９】

ＸＸ＝０２は、フラッシュメモリチップ１３０が故障などにより利用できないエラーを意味する。

【００５０】

ＸＸ＝０３は、第１制御バイト２０１の下位４ビットが現在のアクセスモードに合致しないエラーを意味する。

【００５１】

ＸＸ＝０４は、第２制御バイト２０２で要求された次回のアクセスモードが不正であるエラーを意味する。

【００５２】

図３を参照しながら、ＩＣカードチップ１５０内のアプレットが、セキュアデータエリア１３３にアクセスを開始するときの処理の流れ、およびライト／リード転送コマンドによってそこに対するアクセスを実行するときの処理の流れを説明する。

【００５３】

ホスト機器１６０はMMC１１０にセキュアライトコマンドを発行し（３０１）、セキュアライトデータ５０１を入力する（３０２）。コントローラチップ１２０は、セキュアライトデータ５０１からＩＣカードコマンドのコマンドＡＰＤＵ５０２を抽出し（３０３）、それを用いてＩＣカードチップ１５０にＩＣカードコマンドを発行する（３０４）。

【００５４】

ＩＣカードチップ１５０は、そのＩＣカードコマンドを受信し（３０５）、セキュアデータエリア１３３へのアクセスを要求するＩＣカードレスポンス２００を作成し、それを返信する（３０６）。コントローラチップ１２０は、このレスポンスを受信し、そのＳＷ１バイト２０５とＳＷ２バイト２０６が９０ＦＦｈであるかを調べる（３０７）。９０ＦＦｈでないならばステップ３０８に移る。９０ＦＦｈであるならば、第１制御バイト２０１の上位４ビットが０００１（アクセス開始要求）であるかを調べる（３１２）。０００１でないならばステップ３２０に移る。０００１であるならば、管理テーブル１３６がロックされているか調べる（３１３）。アンロックされているならばステップ３０８に移る。ロックされているならば、後続出力データ２０３に含まれるＡＩＤで管理テーブル１３６上のＡＩＤ１３７を検索する（３１４）。一致するＡＩＤを検出したならば（３１５）、コントローラチップ１２０はアクセス開始要求を承認し、ステップ３１６に移る。検出しなければアクセス開始要求を却下し、ステップ３０８に移る。ステップ３１６では、検出したＡＩＤ１３７に対応するセキュアデータブロックを選択し、それをアクティブにする。さらに、対応する転送コマンドコード１

３８を取得する（３１７）。そして、第１制御バイト２０１の下位４ビットを調べて、開始するアクセスモードを取得し（３１８）、そのアクセスモードに応じて図２ｂに示すようなライト／リード転送コマンドを作成する（３１９）。その後、ステップ３０４に戻り、ＩＣカードチップ１５０にライト／リード転送コマンドを発行する。

【００５５】

ステップ３２０では、第１制御バイト２０１の上位４ビットが００１０（アクセス実行要求）であるかを調べる。００１０でないならばステップ３０８に移る。００１０であるならば、アクティブなセキュアデータブロックが存在するか、また第１制御バイト２０１の下位４ビットがコントローラチップ１２０の認知するアクセスモードに合致するかを調べる（３２１）。いずれかが偽ならばステップ３０８に移る。両者とも真ならば、アクセス実行を承認し、後続出力データ２０３に含まれるレコード番号を取得する（３２２）。そして、そのレコード番号の指示するデータに対してライト／リードを実行する（３２３）。このとき、ライトモードの場合は、後続出力データ２０３に含まれる１２８バイトのデータをライトする。次に、そのアクセスの結果を示すコードを２１２または２２２に設定する（３２４）。そして、第１制御バイト２０１の下位４ビットを調べて、次回のアクセスモードを取得し（３１８）、そのアクセスモードに応じて図２ｂまたは図２ｃに示すようなライト／リード転送コマンドを作成する（３１９）。その後、ステップ３０４に戻り、ＩＣカードチップ１５０にライト／リード転送コマンドを発行する。

【００５６】

ステップ３０８では、ＩＣカードチップ１５０が返信したレスポンスＡＰＤＵ５１２からセキュアリードデータ５１１を作成する。ステップ３０８に至ることによって、セキュアデータエリア１３３へのアクセスは終了する。この後、ホスト機器１６０はセキュアリードコマンドを発行し（３０９）、コントローラチップ１２０はセキュアリードデータ５１１を出力する（３１０）。そして、ホスト機器１６０はセキュアリードデータ５１１を受信する（３１１）。

【００５７】

以上より、ホスト機器１６０から一組のセキュアライト／セキュアリードコマンドをMMC１１０に処理させる間に、ＩＣカードチップ１５０内のアプレットは任意の回数、セキュアデータエリア１３３へアクセスすることができる。

【００５８】

以下、管理エリア１３２に関するアクセスについて説明する。

【００５９】

ホスト機器１６０が管理エリア１３２の情報にアクセスできるように、MMC１１０は、以下の４つの管理コマンドに応じることができる。すなわち、（１）アプレット登録コマンド、（２）アプレット登録解除コマンド、（３）管理テーブルロックコマンド、（４）管理テーブルアンロックコマンドの４つである。（１）は、管理テーブル１３６にセキュアデータエリア１３３を利用するアプレットを登録し、アプレットが利用するセキュアデータブロックを割り当てるコマンド、（２）は、管理テーブル１３６からアプレットの登録情報を削除し、セキュアデータブロックの割り当てを解除するコマンド、（３）は、管理テーブル１３６上の登録情報の変更を禁止するコマンド、（４）は、管理テーブル上１３６の登録情報の変更を許可するコマンドである。これらのコマンドは、一般のセキュリティ処理と同じくセキュアライトコマンドとセキュアリードコマンドのプロトコルによって実施され、コントローラチップ１２０によって処理される。また、その際に入出力されるセキュアライトデータとセキュアリードデータに含まれるＡＰＤＵ（図５における５０２や５１２）を利用して各処理（登録、登録解除、ロック、アンロック）に必要な情報を交換する。

【００６０】

アプレット登録コマンドとアプレット登録解除コマンドでは、ＤａｔａＩｎ５０６にＡＩＤを設定する。このＡＩＤによって登録したいアプレットを指定する。ＡＩＤとセキュアデータブロックとをどのように対応付けるかはコントローラチップ１２０が決定する。ホスト機器２２０はセキュアデータブロックを直接指定できない。

【００６１】

管理テーブルロックコマンドでは、ＤａｔａＩｎ５０６に２５５バイトのパス

ワードを設定する。そのパスワードはパスワードエリア１３５に設定され、ロックフラグ１３４がＦＦｈ（ロック状態）になる。これにより、アプレット登録コマンドとアプレット登録解除コマンドが無効になる。すでにロック状態だった場合は、そのパスワードはパスワードエリア１３５に設定されず、アプレット登録コマンドとアプレット登録解除コマンドは有効のままとなる。

【００６２】

管理テーブルアンロックコマンドでは、ＤａｔａＩｎに２５５バイトのパスワードを設定する。そのパスワードはパスワードエリア１３５に設定された値と一致比較され、一致したならばロックフラグ１３４が００ｈ（アンロック状態）になる。これにより、アプレット登録コマンドとアプレット登録解除コマンドが有効になる。すでにアンロック状態だった場合は、アプレット登録コマンドとアプレット登録解除コマンドは無効のままとなる。

【００６３】

アプレット登録コマンドとアプレット登録解除コマンドが有効な状態（アンロック状態）では、パスワードを知らないホスト機器１６０によって管理テーブル１３６の情報が不正に変更され、あるアプレットが、それ自身がアクセス可能なセキュアデータブロック以外のセキュアデータブロックをライト／リードするという不正アクセスが発生しうる。そこで、コントローラチップ１２０は、ロックフラグ１３４の値が００ｈ（アンロック状態）では、ＩＣカードチップ１５０内で選択されているアプレットがセキュアデータエリアへアクセスするのを許可しない。ホスト機器１６０は、管理テーブル１３６の登録情報の設定／変更後は、管理テーブルロックコマンドにより必ずロックフラグ１３４をＦＦｈに設定しなければならない。

【００６４】

図４を参照しながら、上記４つの管理コマンドの処理の流れを説明する。

【００６５】

ホスト機器１６０はMMC１１０にセキュアライトコマンドを発行し（４０１）、セキュアライトデータ５０１を入力する（４０２）。コントローラチップ１２０は、セキュアライトデータ５０１からＩＣカードコマンドのコマンドＡＰＤ

Ｕ５０２を抽出し（４０３）、それが管理コマンドであるかを調べる（４０４）。管理コマンドならばステップ４０７に移る。一方、管理コマンドでないならば、そのコマンドＡＰＤＵ５０２を用いてＩＣカードチップ１５０にＩＣカードコマンドを発行し（４０５）、ＩＣカードチップ１５０からそのレスポンスを受信し（４０６）、ステップ４２７に移る。

【００６６】

ステップ４０７では、コントローラチップ１２０は、コマンドＡＰＤＵ５０２がアプレット登録コマンドを示すものかを調べる。アプレット登録コマンドならばステップ４１１に移る。さもなくば、それがアプレット登録解除コマンドを示すものかを調べる（４０８）。アプレット登録解除コマンドならばステップ４１２に移る。さもなくば、それが管理テーブルロックコマンドを示すものかを調べる（４０９）。管理テーブルロックコマンドならばステップ４１３に移る。さもなくば、それが管理テーブルアンロックコマンドを示すものかを調べる（４１０）。管理テーブルアンロックコマンドならばステップ４１４に移る。さもなくば、ステップ４２５に移る。

【００６７】

ステップ４１１では、ロックフラグ１３４を見て、管理テーブル１３６がアンロック状態かを調べる。ロック状態ならばステップ４２５に移る。アンロック状態ならば、ＤａｔａＩｎ５０６内のＡＩＤと同一のものが既に登録されているＡＩＤ１３７の中に存在するか調べる（４１５）。存在していればステップ４２５に移る。存在しなければ、管理テーブル１３６上に空きがあるか（つまり、まだ割り当てられていないセキュアデータブロックが存在するか）を調べる（４１６）。空きがなければステップ４２５に移る。空きがあれば、そのセキュアデータブロックに対応するＡＩＤ１３７と転送コマンドコード１３８に、ＤａｔａＩｎ５０６に含まれるＡＩＤと転送コマンドコードを設定する（４１７）。これにより、ＡＩＤで示されたアプレットがそのセキュアデータブロックの利用権を獲得する。そして、ステップ４２６に移る。

【００６８】

ステップ４１２では、ロックフラグ１３４を見て、管理テーブル１３６がアン

ロック状態かを調べる。ロック状態ならばステップ４２５に移る。アンロック状態ならば、ＤａｔａＩｎ５０６内のＡＩＤで、登録されている全てのＡＩＤ１３７の中を検索する（４１８）。一致するＡＩＤを検出したならば（４１９）、管理テーブル１３６上からそのＡＩＤ１３７とそれに対応する転送コマンドコード１３８を削除する（４２０）。一致するＡＩＤを検出しなければステップ４２５に移る。これにより、ＡＩＤで示されたアプレットがそのセキュアデータブロックの利用権を失う。そして、ステップ４２６に移る。

ステップ４１３では、ロックフラグ１３４を見て、管理テーブル１３６がアンロック状態かを調べる。ロック状態ならばステップ４２５に移る。アンロック状態ならば、ロックフラグ１３４にＦＦｈを設定し（４２１）、管理テーブル１３６をロック状態にする。ＤａｔａＩｎ５０６内のパスワードをパスワードエリア１３５に設定する（４２２）。そして、ステップ４２６に移る。

【００６９】

ステップ４１４では、ロックフラグ１３４を見て、管理テーブル１３６がアンロック状態かを調べる。アンロック状態ならばステップ４２５に移る。ロック状態ならば、ＤａｔａＩｎ５０６内のパスワードがパスワードエリア１３５に設定したものと一致するかを調べる（４２３）。一致しないならば、ステップ４２５に移る。一致するならば、ロックフラグ１３４に００ｈを設定し（４２４）、管理テーブル１３６をアンロック状態にする。そして、ステップ４２６に移る。

【００７０】

ステップ４２５では、管理コマンドの処理でエラーが発生したことをホスト機器１６０に示すため、エラー内容を示すステータスコードを含むレスポンスＡＰＤＵ５１２を作り、ステップ４２７に移る。ステップ４２６では、管理コマンドの処理が正常に終了したことをホスト機器１６０に示すため、正常終了（例えば、９０００ｈ）というステータスコードを含むレスポンスＡＰＤＵ５１２を作り、ステップ４２７に移る。

【００７１】

ステップ４２７では、レスポンスＡＰＤＵ５１２からセキュアリードデータ５１１を作成する。この後、ホスト機器１６０はセキュアリードコマンドを発行し

（４２８）、コントローラチップ１２０はセキュアリードデータ５１１を出力する（４２９）。そして、ホスト機器１６０はセキュアリードデータ５１１を受信する（４３０）。

【００７２】

尚、本発明は、カード形式以外の記憶装置にも適用可能である。

【００７３】

【発明の効果】

本発明によれば、ＩＣカードチップのアプレットごとにメモリの異なるブロックを割り当てることにより、ＩＣカードチップのアプレット間のデータ干渉、即ち、あるアプレットに割り当てられたメモリが他のアプレットにもアクセスされてデータが侵害されることを抑制できるという効果を奏する。

【図面の簡単な説明】

【図１】本発明を適用したＭＭＣの内部構成を示す図である。

【図２】コントローラチップとＩＣカードチップとの間のＩＣカードコマンドおよびＩＣカードレスポンスの構造を示す図である。

【図３】ＩＣカードチップからの要求に応じてフラッシュメモリチップ上のセキュアデータエリアに対するデータの読み書きを実行するフローチャートである。

【図４】ＩＣカードチップからの要求に応じてフラッシュメモリチップ上の管理エリアに対するアプレットの登録およびその解除、また登録情報のロックおよびアンロックを実行するフローチャートである。

【図５】セキュアライトデータとセキュアリードデータの構成図である。

【符号の説明】

１１０…ＭＭＣ、１２０…コントローラチップ、１３６…管理テーブル、１４０…ＭＭＣ外部端子、１５０…ＩＣカードチップ、１６０…ホスト機器。

【書類名】図面

【図１】

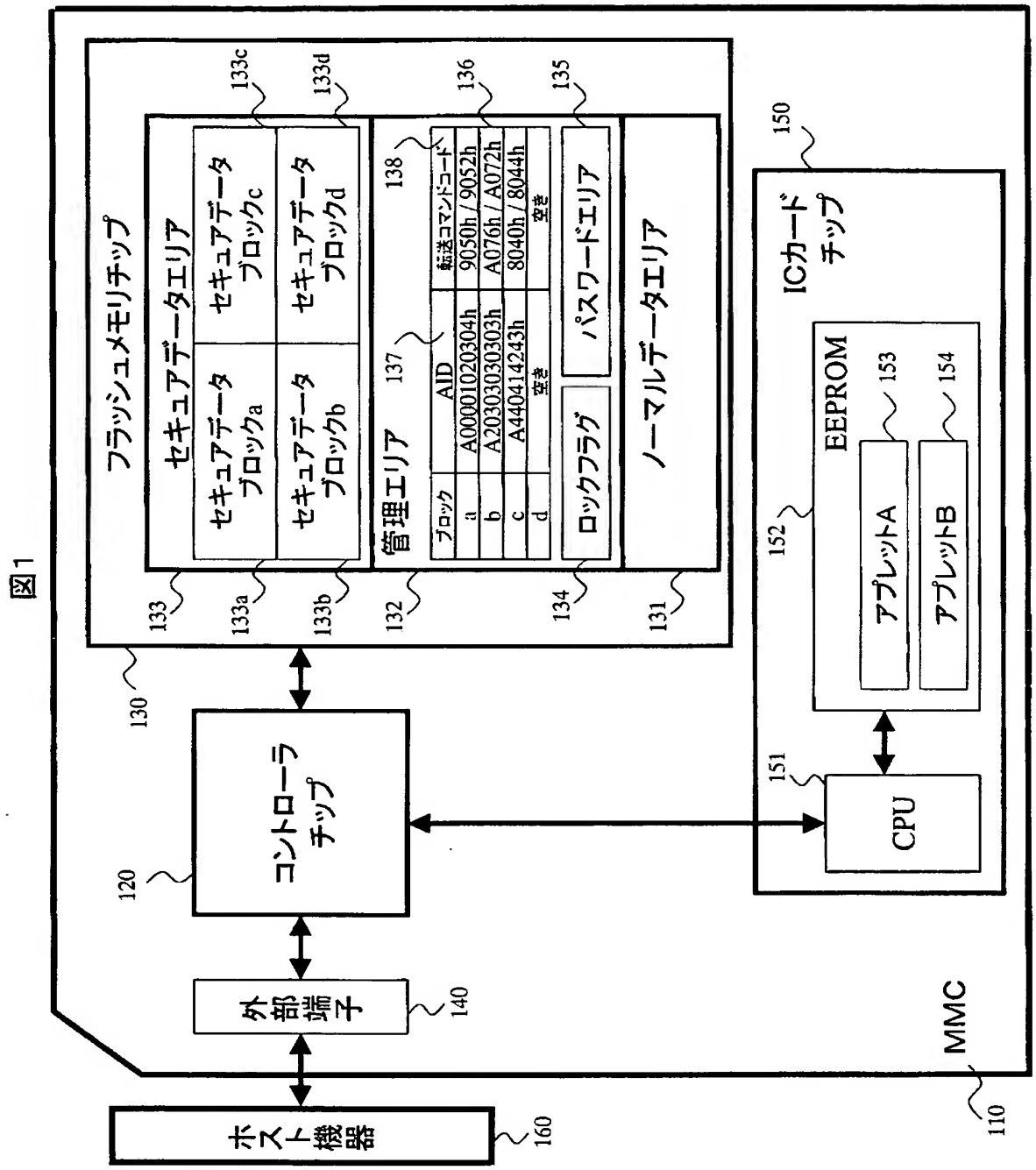


図1
MMC
110
フラッシュメモリチップ
130
セキュアデータエリア
133
セキュアデータ ブロックa
133a
セキュアデータ ブロックb
133b
セキュアデータ ブロックc
133c
セキュアデータ ブロックd
133d
管理エリア
132
137
AID
138
転送コマンドコード
136
ブロック
a
b
c
d
A00001020304h
A20303030303h
A4404142 43h
空き
9050h / 9052h
A076h / A072h
8040h / 8044h
空き
ロックフラグ
134
パスワードエリア
135
ノーマルデータエリア
131
コントローラ チップ
120
外部端子
140
ホスト機器
160
ICカード チップ
150
CPU
151
EEPROM
152
アプレットA
153
アプレットB
154

【図２】

図2

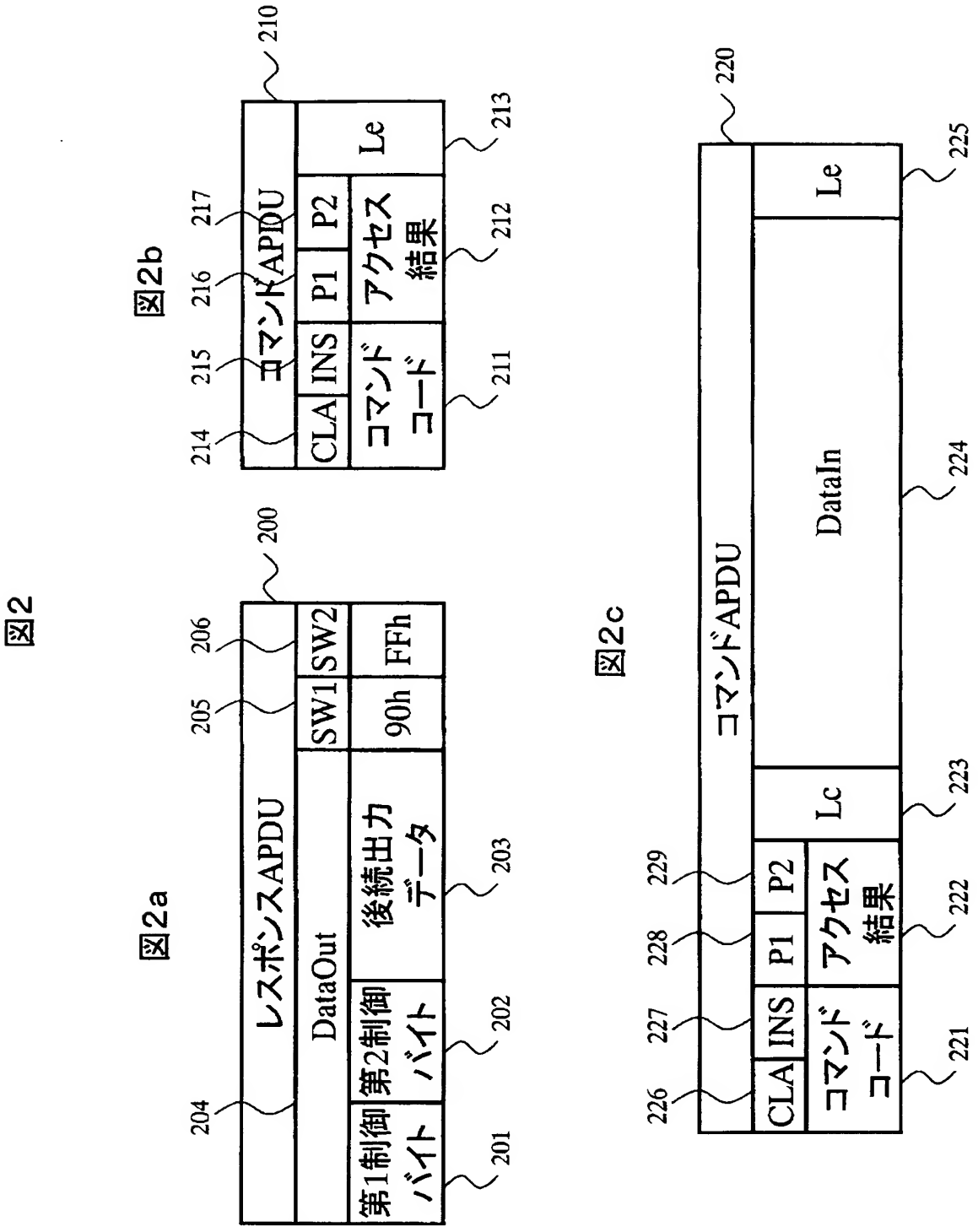


図2a
レスポンスAPDU
DataOut
第1制御バイト
第2制御バイト
後続出力データ
SW1
SW2
90h
FFh
200
201
202
203
204
205
206
図2b
コマンドAPDU
CLA
INS
P1
P2
コマンドコード
アクセス結果
Le
210
211
212
213
214
215
216
217
図2c
コマンドAPDU
CLA
INS
P1
P2
コマンドコード
アクセス結果
Lc
DataIn
Le
220
221
222
223
224
225
226
227
228
229

【図３】

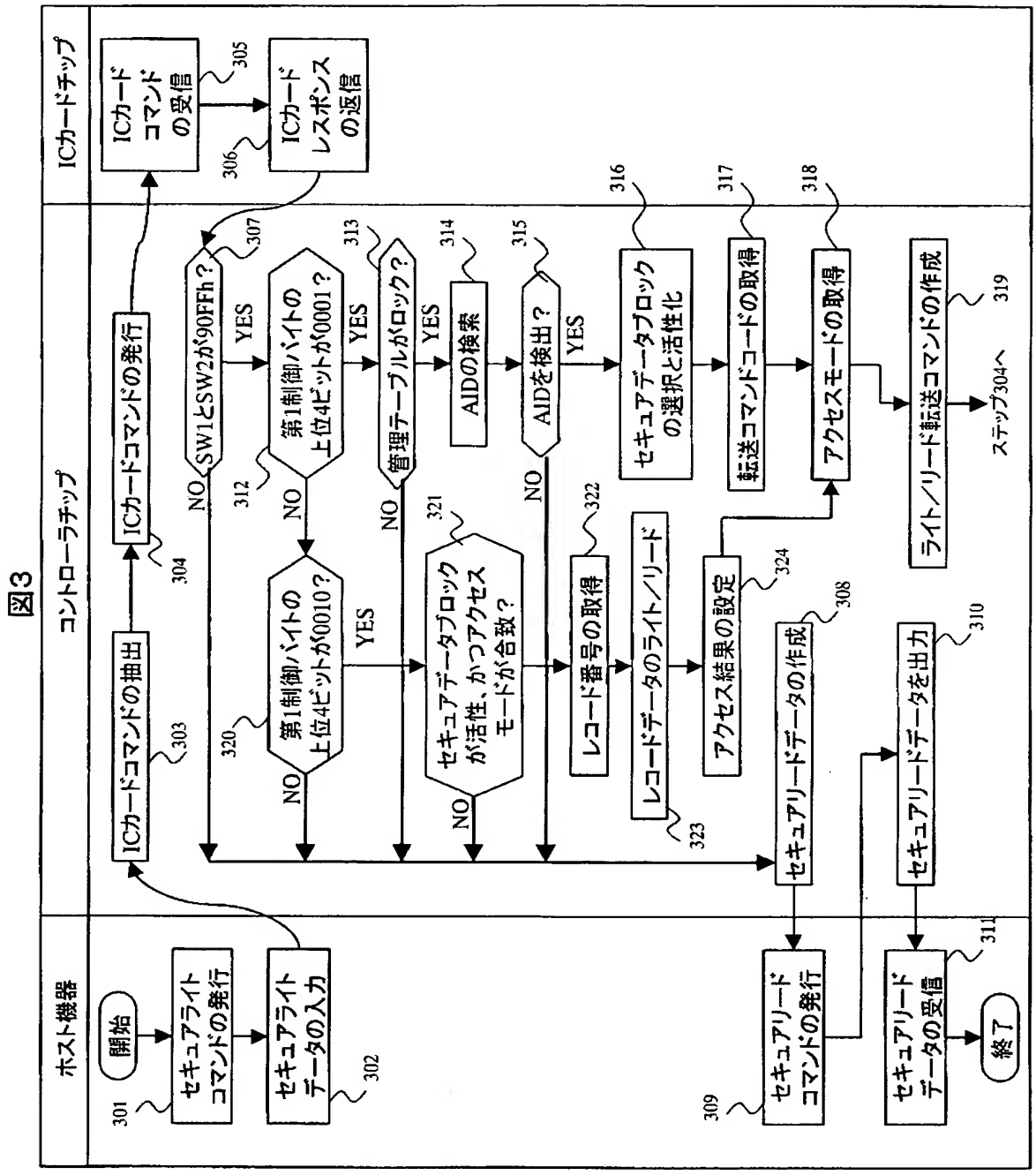


図3
ホスト機器
コントローラチップ
ICカードチップ
開始
301
セキュアライトコマンドの発行
セキュアライトデータの入力
302
ICカードコマンドの抽出
303
ICカードコマンドの発行
304
ICカードコマンドの受信
305
ICカードレスポンスの返信
306
SW1とSW2が90FFh？
307
YES
NO
第1制御バイトの上位4ビットが0001？
312
管理テーブルがロック？
313
AIDの検索
314
AIDを検出？
315
セキュアデータブロックの選択と活性化
316
転送コマンドコードの取得
317
アクセスモードの取得
318
ライト／リード転送コマンドの作成
319
ステップ304へ
第1制御バイトの上位4ビットが0010？
320
セキュアデータブロックが活性、かつアクセスモードが合致？
321
レコード番号の取得
322
レコードデータのライト／リード
323
アクセス結果の設定
324
セキュアリードデータの作成
308
セキュアリードデータを出力
310
セキュアリードコマンドの発行
309
セキュアリードデータの受信
311
終了

【図４】

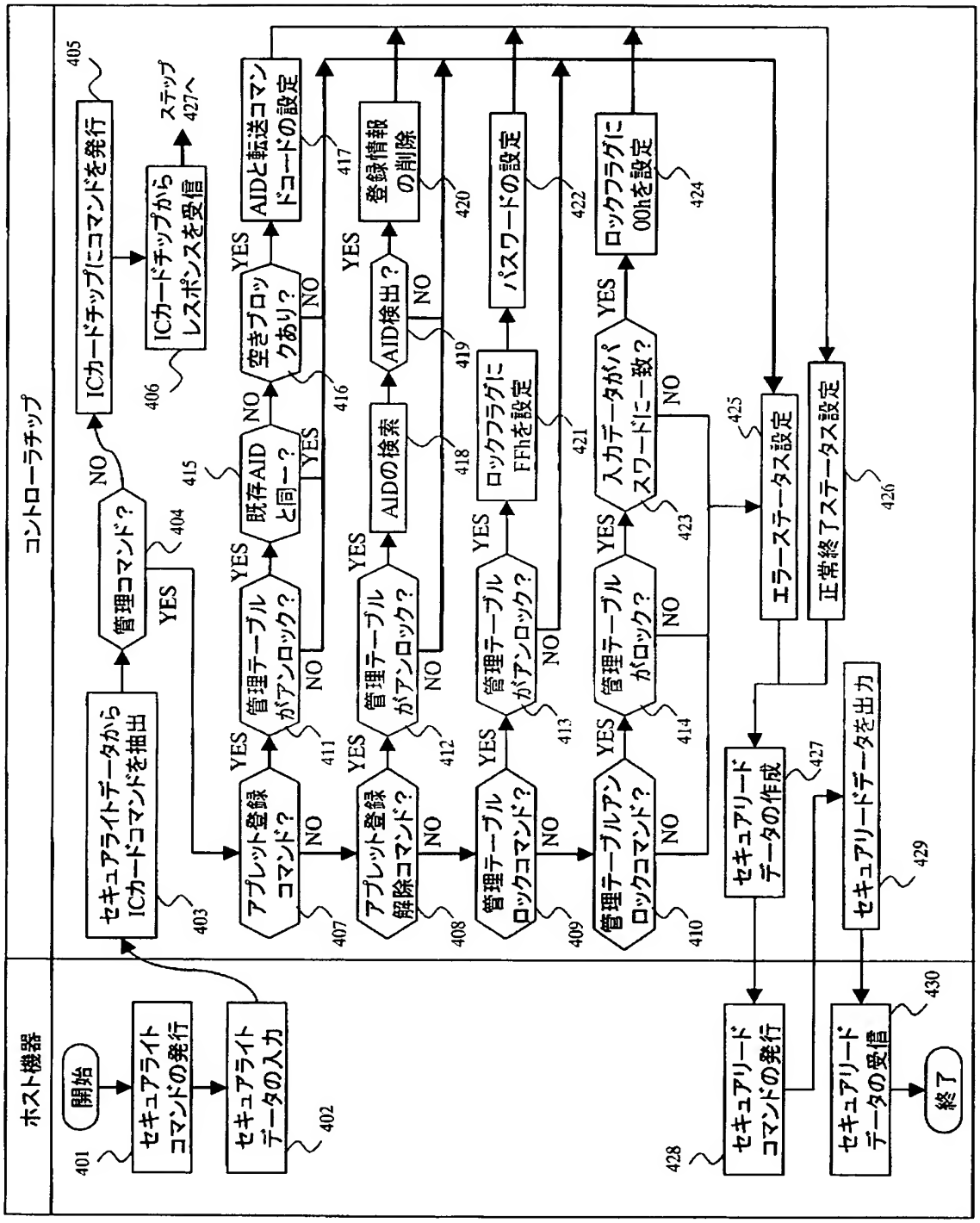
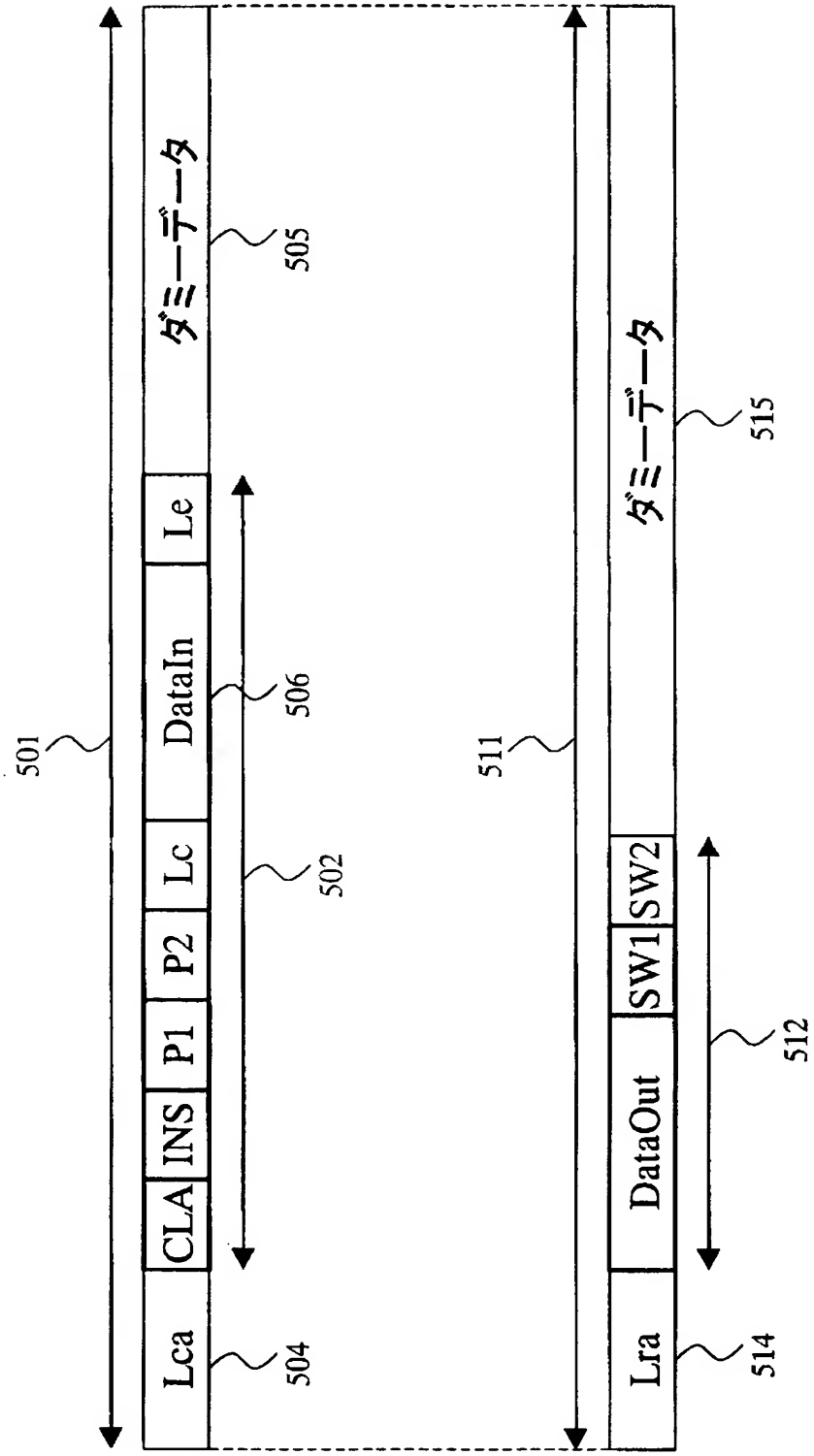


図4
ホスト機器
コントローラチップ
開始
401
セキュアライトコマンドの発行
セキュアライトデータの入力
402
セキュアライトデータからICカードコマンドを抽出
403
管理コマンド？
404
YES
NO
ICカードチップにコマンドを発行
405
ICカードチップからレスポンスを受信
406
ステップ427へ
アプレット登録コマンド？
407
YES
NO
管理テーブルがアンロック？
411
YES
NO
既存AIDと同一？
415
YES
NO
空きブロックあり？
416
YES
NO
AIDと転送コマンドコードの設定
417
アプレット登録解除コマンド？
408
YES
NO
管理テーブルがアンロック？
412
YES
NO
AIDの検索
418
AID検出？
419
YES
NO
登録情報の削除
420
管理テーブルロックコマンド？
409
YES
NO
管理テーブルがアンロック？
413
YES
NO
ロックフラグにFFhを設定
421
パスワードの設定
422
管理テーブルアンロックコマンド？
410
YES
NO
管理テーブルがロック？
414
YES
NO
入力データがパスワードに一致？
423
YES
NO
ロックフラグに00hを設定
424
エラーステータス設定
425
正常終了ステータス設定
426
セキュアリードデータの作成
427
セキュアリードデータを出力
429
セキュアリードコマンドの発行
428
セキュアリードデータの受信
430
終了

【図５】

図5


501
CLA
INS
P1
P2
Lc
DataIn
Le
ダミーデータ
505
506
502
504
Lca
511
SW1
SW2
DataOut
ダミーデータ
515
512
514
Lra

【書類名】　要約書

【要約】

【課題】

ＩＣカードチップのアプレット間のデータ干渉、即ち、一のアプレットに割り当てられたメモリが他のアプレットにもアクセスされてデータが侵害されることを抑制する。

【解決手段】

本発明は、フラッシュメモリチップ１３０と、ＩＣカードチップ１５０と、ホストからの要求に応じてフラッシュメモリチップ及びＩＣカードチップへのデータの読み書きを制御するコントローラチップ１２０とを備え、フラッシュメモリチップは、ホスト機器からのデータを記憶するためのノーマルデータエリア１３１とＩＣカードチップからのデータを記憶するためのセキュアデータエリア１３３を有し、さらに、セキュアデータエリア１３３は、アプレット１５３，１５４ごとに割り当てられたセキュアデータブロック１３３ａ，１３３ｂ，１３３ｃ，１３３ｄに分割される。

【選択図】図１

認定・付加情報

特許出願の番号	特願２００３－０２８９９８
受付番号	５０３００１８７６８５
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　２月　７日

＜認定情報・付加情報＞

【提出日】　平成15年 2月 6日

次頁無

【書類名】　出願人名義変更届（一般承継）
【あて先】　特許庁長官　殿
【事件の表示】
　【出願番号】　特願2003- 28998
【承継人】
　【識別番号】　503121103
　【氏名又は名称】　株式会社ルネサステクノロジ
【承継人代理人】
　【識別番号】　100080001
　【弁理士】
　【氏名又は名称】　筒井　大和
【提出物件の目録】
　【包括委任状番号】　0308729
　【物件名】　承継人であることを証明する登記簿謄本　1
　　【援用の表示】　特許第３１５４５４２号　平成１５年４月１１日付け提出の会社分割による特許権移転登録申請書　を援用する
　【物件名】　権利の承継を証明する承継証明書　1
　　【援用の表示】　特願平１－２５１８８９号　同日提出の出願人名義変更届（一般承継）を援用する
【プルーフの要否】　要

認定・付加情報

特許出願の番号	特願２００３－０２８９９８
受付番号	５０３０１４０３５１５
書類名	出願人名義変更届（一般承継）
担当官	小野寺　光子　　１７２１
作成日	平成１５年１１月　４日

＜認定情報・付加情報＞

【提出日】　平成15年 8月26日

特願２００３－０２８９９８

出　願　人　履　歴　情　報

識別番号　　［０００００５１０８］

１．変更年月日　　１９９０年　８月３１日
［変更理由］　　新規登録
住　所　　東京都千代田区神田駿河台４丁目６番地
氏　名　　株式会社日立製作所

特願２００３－０２８９９８

出　願　人　履　歴　情　報

識別番号　［５０３１２１１０３］

１．変更年月日　２００３年　４月　１日
［変更理由］　新規登録
住　所　東京都千代田区丸の内二丁目４番１号
氏　名　株式会社ルネサステクノロジ